AMENDMENTS TO THE CLAIMS

Please cancel claims 28-55, 65 and 84-110 without prejudice.

Kindly amend claims 1-27, 56-58, 68-71, 74-75 and 78-82 as directed below in the following detailed listing of all claims.

1. (Currently amended): ~~An apparatus in a microprocessor, for accomplishing cryptographic operations~~An instruction for employment by a device, the instruction directing the device to perform a cryptographic operation, the instruction comprising:

an opcode field, configured to prescribe that the device accomplish the cryptographic operation as further specified within a control word stored in a memory; and

a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the instruction is to be accomplished on a plurality of blocks of input data.

~~translation logic, configured to receive a cryptographic instruction from a source therefrom, wherein said cryptographic instruction prescribes one of the cryptographic operations, and configured to translate said cryptographic instruction into a sequence of micro instructions specifying sub-operations required to accomplish said one of the cryptographic operations; and~~

~~execution logic, operatively coupled to said translation logic, configured to receive said sequence of micro instructions, and configured to perform said sub-operations.~~

2. (Currently amended): The ~~apparatus~~ instruction as recited in claim 1, wherein ~~said one of~~ the cryptographic operations is accomplished at the level of system privileges afforded to application programs.

3. (Currently amended): The ~~apparatus~~ instruction as recited in claim 1, wherein ~~said one of~~ the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

4. (Currently amended): The ~~apparatus~~ instruction as recited in claim 1, wherein ~~said one of~~ the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

5. (Currently amended): The ~~apparatus~~ instruction as recited in claim 1, wherein ~~said one of~~ the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

6. (Currently amended): The ~~apparatus~~ instruction as recited in claim 1, wherein ~~said cryptographic~~the instruction prescribes a block cipher mode to be employed in accomplishing ~~said one of~~ the cryptographic operations.

7. (Currently amended): The ~~apparatus~~ instruction as recited in claim 6, wherein said block cipher mode comprises electronic code book (ECB) mode.

8. (Currently amended): The instruction ~~apparatus~~ as recited in claim 6, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

9. (Currently amended): The instruction ~~apparatus~~ as recited in claim 6, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

10. (Currently amended): The instruction ~~apparatus~~ as recited in claim 6, wherein said block cipher mode comprises output feedback (OFB) mode.

11. (Currently amended): The instruction ~~apparatus~~ as recited in claim 1, wherein ~~said~~ the ~~cryptographic~~ instruction prescribes that ~~said one of~~ the cryptographic operations be accomplished on a plurality of text blocks.

12. (Currently amended): The instruction ~~apparatus~~ as recited in claim 1, wherein ~~said~~ the ~~cryptographic~~ instruction is prescribed according to the x86 instruction format.

13. (Currently amended): The instruction ~~apparatus~~ as recited in claim 1, wherein ~~said cryptographic~~the instruction implicitly references a plurality of registers within the ~~microprocessor~~device.

14. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of a plurality of input text blocks upon which ~~said one of~~ the cryptographic operations is to be accomplished.

15. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing ~~said one of~~ the cryptographic operations upon a plurality of input text blocks.

16. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

17. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing ~~said one of~~ the cryptographic operations.

18. (Currently amended): The instruction ~~apparatus~~ as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key.

19. (Currently amended): The instruction ~~apparatus~~ as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key schedule.

20. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing ~~said one of~~ the cryptographic operations.

21. (Currently amended): The instruction ~~apparatus~~ as recited in claim 13, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of ~~a~~ said control word for use in accomplishing ~~said one of~~ the cryptographic operations, wherein said control word prescribes cryptographic parameters for ~~said one of~~ the cryptographic operations.

22. (Currently amended): The instruction ~~apparatus~~ as recited in claim 21, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether ~~said one of~~ the cryptographic operations is an encryption operation or a decryption operation.

23. (Currently amended): The instruction ~~apparatus~~ as recited in claim 1, wherein ~~said execution logic~~ the device comprises:

a cryptography unit, configured to ~~receive a first plurality of said sequence of micro-instructions, and configured to~~ execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by ~~a~~ said control word ~~that is provided to said cryptography unit~~.

24. (Currently amended): The instruction ~~apparatus~~ as recited in claim 23, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of a plurality of input text blocks according to ~~said one of~~ the cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

25. (Currently amended): The instruction ~~apparatus~~ as recited in claim 23, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more input text blocks.

26. (Currently amended): The instruction ~~apparatus~~ as recited in claim 23, wherein said ~~execution logic~~ device further comprises:

an integer unit, coupled in parallel with said cryptography unit, configured to ~~receive a second plurality of said sequence of micro instructions, and configured to~~ execute a plurality of integer operations that are required to accomplish ~~said one of~~ the cryptographic operations.

27. (Currently amended): The instruction ~~apparatus~~ as recited in claim 23, wherein ~~said sequence of micro instructions comprises:~~

~~a first micro instruction, configured to~~ said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds.

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Cancelled)

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled)

47. (Cancelled)

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (Cancelled)

53. (Cancelled)

54. (Cancelled)

55. (Cancelled)

56. (Currently amended): An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by logic within a ~~processor~~circuit, wherein said cryptographic instruction prescribes one of the cryptographic operations~~; and~~, said cryptographic instruction comprising:

an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory; and

a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data.

~~execution logic, coupled to said logic, configured to perform said one of the cryptographic operations.~~

57. (Currently amended): The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of ~~a~~ said plurality of ~~plaintext~~ blocks of input data to generate a corresponding plurality of ciphertext blocks.

58. (Currently amended): The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of ~~a~~ said plurality of ~~ciphertext~~ blocks of input data to generate a corresponding plurality of plaintext blocks.

59. (Original): The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

60. (Original): The apparatus as recited in claim 56, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

61. (Original): The apparatus as recited in claim 60, wherein said block cipher mode comprises electronic code book (ECB) mode.

62. (Original): The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

63. (Original): The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

64. (Original): The apparatus as recited in claim 60, wherein said block cipher mode comprises output feedback (OFB) mode.

65. (Cancelled).

66. (Original): The apparatus as recited in claim 60, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

67. (Original): The apparatus as recited in claim 56, wherein said cryptographic instruction implicitly references a plurality of registers within said processor.

68. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of a said plurality of ~~input text~~ blocks of input data upon which said one of the cryptographic operations is to be accomplished.

69. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon ~~a~~ said plurality of ~~input text~~ blocks of input data.

70. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within ~~a~~ said plurality of ~~input text~~ blocks of input data.

71. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

72. (Original): The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key.

73. (Original): The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key schedule.

74. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

75. (Currently amended): The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of ~~a~~ said control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

76. (Original): The apparatus as recited in claim 75, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether said one of the cryptographic operations is an encryption operation or a decryption operation.

77. (Original): The apparatus as recited in claim 56, further comprising:

translation logic, configured to translate said cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish said one of the cryptographic operations.

78. (Currently amended): The apparatus as recited in claim 77, ~~wherein said execution logic comprises~~further comprising:

a cryptography unit, configured to receive a first plurality of said associated micro instructions, and configured to execute a plurality of cryptographic rounds on each of ~~a~~ said plurality of ~~input text~~ blocks of input data to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by ~~a~~ said control word ~~that is provided to said cryptography unit~~.

79. (Currently amended): The apparatus as recited in claim 78, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of ~~a~~ said plurality of ~~input text~~ blocks of input data according to said one of the block cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

80. (Currently amended): The apparatus as recited in claim 79, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more ~~input text blocks~~of said plurality of blocks of input data.

81. (Currently amended): The apparatus as recited in claim 78, ~~wherein said execution logic further comprises:~~further comprising:

an integer unit, coupled in parallel with said cryptography unit, configured to receive a second plurality of said associated micro instructions, and configured to execute a plurality of integer operations that are required to accomplish said one of the cryptographic operations.

82. (Currently amended): The apparatus as recited in claim 78, wherein said associated micro instructions comprise:

a first micro instruction, configured to direct said cryptography unit to load one of said each of said plurality of ~~input text~~ blocks of input data and to perform said plurality of cryptographic rounds.

83. (Original): The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished at the privilege level afforded to application programs.

84. (Cancelled).

85. (Cancelled).

86. (Cancelled).

87. (Cancelled).

88. (Cancelled).

89. (Cancelled).

90. (Cancelled).

91. (Cancelled).

92. (Cancelled).

93. (Cancelled).

94. (Cancelled).

95. (Cancelled).

96. (Cancelled).

97. (Cancelled).

98. (Cancelled).

99. (Cancelled).

100. (Cancelled).

101. (Cancelled).

102. (Cancelled).

103. (Cancelled).

104. (Cancelled).

105. (Cancelled).

106. (Cancelled).

107. (Cancelled).

108. (Cancelled).

109. (Cancelled).

110. (Cancelled).